

(11) Japanese Patent Application Laid-Open No.

8-44643

(43) Laid-Open Date: February 16, 1996

(21) Application No. 6-175125

5 (22) Application Date: July 27, 1994

(71) Applicant: Fujitsu Ltd.

(72) Inventor: Ryusuke Masuoka

(72) Inventor: Hiroyuki Okada

(72) Inventor: Nobuaki Suematsu

10 -----

(54)[Title of the Invention] Gateway Apparatus

(57)[Abstract]

15 [Object]

An object of the present invention is to allow a user to access an external database transparently to the user by using hypertext without using a special client and without sacrificing security.

20 [Constitution]

A link replacing unit for replacing a link in a hypertext and a link changing device for changing the link are provided in a hypertext changing device 4, wherein when the link replacing device receives a
25 hypertext, the link changing device changes link information in accordance with given processing means and then the link replacing device outputs the

hypertext in which the link information has been changed.

[Claims]

5 [Claim 1]

A gateway apparatus comprising a hypertext changing device,

the hypertext changing device including:

link replacing means for replacing a link in a
10 hypertext; and

link changing means for changing the link;

wherein, when the link replacing means receives a hypertext, the link changing means changes link information in the hypertext according to given
15 processing means; and then

the link replacing means outputs the hypertext in which the link information has been changed.

[Claim 2]

A gateway apparatus comprising a hypertext
20 generating device,

the hypertext generating device including:

hypertext generating means for converting information into a hypertext; and

link setting means for generating a link;

25 wherein the hypertext generating means converts obtained information into a hypertext;

the link setting means changes link information according to given processing means; and then

the hypertext generating means outputs the hypertext in which the link information has been
5 changed.

[Claim 3]

The gateway apparatus according to claim 1 or 2, wherein means for adding information for re-accessing the same gateway is provided as the given processing
10 means for changing link information.

[Claim 4]

The gateway apparatus according to claim 1 or 2, wherein means for adding information for re-accessing the same gateway or accessing a different gateway is
15 provided as the given processing means for changing link information.

[Claim 5]

The gateway apparatus according to claim 1 or 2, wherein means for providing information for accessing a
20 different server is provided as the given processing means for changing link information.

[Claim 6]

A gateway apparatus comprising:

a link analyzing device which receives link
25 information and analyzes the link information;

a network services access control device which accesses a server to obtain information on the basis of

access information provided from the link analyzing device;

a hypertext changing device which, if the obtained information is a hypertext, changes the link
5 information in the hypertext according to given processing means; and

a hypertext generating device which, if the obtained information is not a hypertext, converting the obtained information into a hypertext and changing the
10 link information according to given processing means.
[Claim 7]

The gateway apparatus according to claim 6,
wherein means for adding information for re-accessing the same gateway is provided as the given processing
15 means for changing link information.
[Claim 8]

The gateway apparatus according to claim 6,
wherein means for adding information for re-accessing the same gateway or accessing a different gateway is
20 provided as the given processing means for changing link information.
[Claim 9]

The gateway apparatus according to claim 6,
wherein means for providing information for accessing a
25 different server is provided as the given processing means for changing link information.

[Detailed Description of the Invention]

[0001]

[Field of the Invention]

The present invention relates to an apparatus which changes a link in a hypertext or implementing a gateway by a hypertext.

[0002]

Various databases distributed on a network and clients which access the databases have been emerging in recent years. Protocols supporting them include Local File System, FTP, Internet News, TELNET, WAIS, GOPHER, and WWW (World Wide Web) HTTP (Hyper Text Transfer Protocol). In the WWW, particularly, servers using protocols different from those used by clients are accessed directly or through gateways and results of the access are converted to hypertexts and the hypertexts are ultimately presented to users.

[0003]

While various kinds of information can be readily obtained in this way, many organizations such as companies that must ensure the security of information restricts access to external sources. However, as various databases on a network are enhanced, demand for straightforward access to their data is growing.

[0004]

Therefore, there is need for providing users with access to external databases in a manner similar to

accessing internal databases, that is, transparent access, while ensuring required database security.

[0005]

[Prior Art]

5 Terms used herein will be defined first. The term server refers to an entity that provides information to a client accessing the server by using a certain protocol.

[0006]

10 The term client refers an entity that obtains information held by a server by using a certain protocol and is typically implemented by software. The term protocol refers to a set of rules for communication between computers for a certain purpose
15 (such as exchange of a file).

[0007]

Hypertext is a way to present information, in which a number of words in a document works as links and, when such a word is selected, another document
20 which is pointed to by the link is displayed. The document pointed to by a link may be a hypertext, normal text, a still image, video, sound, or any other element.

[0008]

25 A link is a character string that indicates how a document pointed to by the word can be accessed. A link is usually hidden from a user at a client where

information is displayed in hypertext format. A link is a character string containing information such as "which file on which machine is to be accessed with which protocol".

5 [0009]

There are methods in the prior art for directly accessing an external server provided on a network external to an organization from a computer internal to the organization, rather than a computer on the
10 external network.

[0010]

One typical way to ensure the security of the organization in such a case is as follows. The network external to the organization is connected to the
15 internal network through a router. The router places restrictions on protocols that are allowed to pass through the router and the allowed direction and uses the restrictions as a firewall to ensure the internal security of the organization..

20 [0011]

Figures 9 and 10 are schematic diagrams for explaining examples of the conventional art. A first example of the conventional art shown in Figure 9 will be described below. A network 11 internal to an
25 organization in Figure 9 includes a compute 14 which is used by a user 13. Connected onto a network 12 external to the organization are computers 16 and

servers (not shown) which use various protocols such as ETP, TELNET, WAIS, GOPHER, and HTTP. The internal network 11 and the external network 12 are interconnected through a router 15 which allows only
5 limited protocols to pass through it.
[0012]

A way to provide access to external entities in such an environment is to allow some computers (only one of them is shown) provided on a network external to
10 the organization to be accessed from the organization through the use of a certain protocol such as TELNET or ETP. If a user 13 using a computer 14 on the network internal to the organization wants to access an external machine, the user first access a computer 16
15 provided on the external network 12 from the computer, which is a machine internal to the organization, through a router 15 by using TELNET, for example, and then accesses to the external machine by using any of various protocols to which the protocol is converted on
20 the computer 16 to obtain information.
[0013]

Another way to provide access to entities external to an organization while ensuring the security in the organization is shown in Figure 10 as a second example
25 of the conventional art. The example will be described below with respect to Figure 10. In Figure 10, the

same elements as those in Figure 9 are denoted by the same reference numerals.

[0014]

In Figure 10, a new protocol, ZZZ (which is a
5 provisional name) is allowed to pass through a router
15. A computer 14, which is a client that uses a
protocol that cannot pass through the router 15, such
as GOPHER or HTTP, is changed to a special client 17
that uses the protocol ZZZ. Also, a ZZZ server 18,
10 which is a gateway apparatus, is provided in a network
12 external to the organization.

[0015]

If a user 13 wants to access an external machine
from a network 11 internal to the organization, the
15 user 13 first accesses the ZZZ server running on the
computer 16 on the external network 12 through the
router 15 by using the protocol ZZZ. Then, the ZZZ
server 18, on behalf of the client 17, accesses a
GOPHER or HTTP server, for example, on the external
20 network 12 and returns the server's information to the
client 17.

[0016]

[Problems to be Solved by the Invention]

The conventional-art techniques described above
25 have the following problems. The technique that uses a
computer 16 on an external network 12 as in the first
example of the conventional art is complex because it

involves procedures such as a login procedure for first
accessing the computer 16. Another drawback is that if
a user wants to communicate with an external server
from the user's computer 14 on the network internal to
5 the organization by directly using a given protocol,
the user cannot use an ordinary client to do so. For
example, a user who wants to use a window-based client
that displays graphics on the user's computer 14 cannot
use the client because the router 15 allows only
10 character-base protocols such as TELNET to pass through
it.

[0017]

The conventional technique that uses a special
client 17 such as the protocol ZZZ as in the second
15 example allows a user to use a client on the user's
computer. However, the client cannot readily be used.
The ordinary client to be used must be changed to a
special client 17 capable of performing communications
using a special protocol, ZZZ.

20 [0018]

An object of the present invention is to provide
access to an external database by using a hypertext
transparently to users, without using a special client
and without sacrificing security.

25 [0019]

[Means for Solving the Problems]

To solve the problems, the present invention is configured as follows. Figure 1 is a diagram for explaining the principle of the present invention. Provided in a gateway apparatus 1 in Figure 1 are a link analyzing device 2 which analyzes link information, a network services access control device 3 which accesses various network servers to obtain specified information, a hypertext changing device 4 which changes the hypertext of obtained information, and a hypertext generating device 5 which converts obtained information into hypertext.

[0020]

[Operation]

Operation of the present invention based on the configuration described above will be described with respect to Figure 1. First, the link analyzing device 2 receives information about a link. The link analyzing device 2 analyzes the link, converting the information into access information for making access, and provides the access information to the network services access control device 3. The network services access control device 3 accesses various network servers according to the access information and obtains information specified in the access information. If the obtained information is a hypertext, the network services access control device 3 provides the hypertext to the hypertext changing device 4. The hypertext

changing device 4 outputs a hypertext in which the link information in the obtained information is rewritten (modified) according to a given processing method in such a manner that the gateway apparatus 1 or another gateway apparatus or another server is accessed.

5 [0021]

If the obtained information is not a hypertext, the network services access control device 3 provides the obtained information to the hypertext generating device 5. Then, the hypertext generating device 5 outputs a hypertext in which the link information in the obtained information is set in such a manner as to access the gateway apparatus 1 or another gateway apparatus or another server.

10 [0022]

Provision of the gateway apparatus 1 on the external network 12 enables a computer on a network internal to an organization to access resources on the external network by using a client which is based on ordinary hypertext without scarifying security.

15 [0023]

[Embodiments]

Embodiments of the present invention will be described with respect to Figures 2 to 8. Like elements are labeled with like reference numerals throughout the drawings.

20 [0024]

Figure 2 is a block diagram of a gateway apparatus in an embodiment of the present invention. A network controller 7 controls communications performed over a network. An access monitor and control device 6
5 monitors the network controller 7 to see whether there is access.

[0025]

If there is access from a client, the access monitor and control device 6 provides link information
10 provided by the client to the gateway apparatus 1. The gateway apparatus 1 returns a hypertext having a special link to the access monitor and control device 6. With this, the access monitor and control device 6 controls the network controller 7 to return the hyper
15 text to the accessing client.

[0026]

In this case, a link in the hypertext can be written in such a manner that a target pointed to by the original link is accessed from the gateway
20 apparatus 1 after the gateway is re-accessed. With this, the gateway will be automatically re-accessed when a user using the client selects the link.

[0027]

Figure 3 is a diagram for explaining a hypertext
25 changing device of the gateway apparatus 1. Provided in the hypertext changing device 4 are a link replacing unit 41 and a link changing unit 42.

[0028]

A process performed when the hypertext changing device 4 receives a hypertext as an input will be described below. First, the link replacing unit 41
5 receives a hypertext. The link replacing unit 41 extracts a link from the hypertext and provides it to the link changing unit 42. The link changing unit 42 converts the link according to a predetermined processing method (so that the gateway 1 is accessed,
10 for example) and provides the changed link to the link replacing unit 41.

[0029]

The link replacing unit 41 replaces the extracted original link in the hypertext with the changed link
15 and outputs the resulting hypertext. Figure 4 is a diagram for explaining a hypertext generating device of the gateway apparatus. Provided in the hypertext generating device 5 are a hypertext generating unit 51 and a link setting unit 52.

20 [0030]

A process performed when the hypertext generating device 5 receives obtained information as an input will be described below. The hypertext generating unit 51 receives obtained information in various formats such
25 as FTP and GOPHER. The hyper text generating unit 51 converts the information, excluding a link, into a hypertext in an ordinary manner. When generating the

link portion, the hypertext generating unit 51 provides a required control signal (information) to the link setting unit 52.

[0031]

5 The link setting unit 52 generates a link according to a predetermined processing method and provides the link to the hypertext generating unit 51. Then, the hypertext generating unit 51 integrates the link into the hypertext in an ordinary way and outputs
10 the resulting hypertext.

[0032]

For example, if he obtained information is (protocol A + server A + additional information), and if the link setting unit 52 is to rewrite the
15 information so that the gateway apparatus 1 is accessed, the link setting unit 52 adds link information such that

protocol + gateway + (protocol A + server + additional information).

20 [0033]

The added link information is hidden from and transparent to the user of the client. Accordingly, the user feels like the user can access servers on the external network from the network internal to the
25 organization smoothly as if the user were running the client on the external network.

[0034]

Figure 5 is a flowchart of an embodiment of the present invention. Operation of the gateway apparatus 1 will be described below with respect to the flowchart in Figure 5. S1 to S9 are the numbers of steps.

5 [0035]

First, the access monitor and control device 6 determines whether there is access from a client (S1). If there is access from a client, the access monitor and control device 6 receives link information and provides it to a link analyzing device 2 (S2). The link analyzing device 2 extracts access information and provides it to the network services access control device 3 (S3). The network services access control device 3 obtains specified information on the basis of the access information through a network controller 7 (S4).

[0036]

The network services access control device 3 determines whether or not the obtained information is a hypertext (S5). If the obtained information is a hypertext (Yes), the network services access control device 3 provides the obtained information (hypertext) to the hypertext changing device 4, which in turn changes the obtained information according to a predetermined process (S6). If it is determined at step S5 that the obtained information is not a hypertext (No), the various network services access

control device 3 provides the obtained information to the hypertext generating device 5, which then changes the link information ordinarily generated, according to a predetermined process, and outputs the hypertext (S7).

5 [0037]

The hypertext processed at step S6 or S7 is provided to the access monitor and control device 6 (S8). The access monitor and control device 6 returns the hypertext to the client through the network controller 7 (S9).

[0038]

Figure 6 is a diagram for explaining server access in an embodiment. The server access will be described below with respect to Figure 6. Provided in an external network 12 in Figure 6 are a gateway apparatuses 1a, 1b, and servers 20 to 22. Provided in a network 11 internal to an organization are a gateway apparatus 1c, a computer 14, and servers 23, 24. A router 15 interconnects the internal network 11 and the external network 12 and allows only limited protocols such as TELNET, FTP, and HTTP to pass through it.

20

[0039]

The gateway apparatus 1a is provided on the external network 12 in order to allow a user 13 to access an external server 20 from the computer 14 on the internal network 11 while ensuring security. The router 15 allows the HTTP protocol, which is a protocol

25

for exchanging hypertexts, to pass through it from the internal network 11, in addition to the protocols (for example TELNET and ETP) that the router 15 usually allows to pass through it.

5 [0040]

Therefore, once a resource on the server 20 on the external network is accessed through the gateway apparatus 1a, all results of access are returned as hypertexts and links are set so that the gateway apparatus 1a is always accessed. Because links are set in such a manner that the gateway apparatus 1a is accessed every time the access process is performed subsequently, the gateway apparatus 1a is accessed first whenever the client user 13 selects the link.

15 [0041]

If a number of gateway apparatuses 1a of this type (for example gateway apparatus 1b) are provided on the external network 12, load can be distributed among the gateway apparatuses 1a, 1b by selecting one of the gateway apparatuses appropriately and describing it in links.

[0042]

For example, a target of an original link may be analyzed and the gateway apparatus closes to the linked-to target may be selected. Alternatively, depending on a load on a gateway apparatus 1a, another gateway apparatus 1b may be selected. Or, a gateway

apparatus may be selected at random (for example, using random numbers). Or alternatively, gateway apparatus having a less load may be selected through communication between the gateways.

5 [0043]

Furthermore, a gateway that is more than a gateway for merely ensuring security can be implemented as follows. Information about resources at a number of locations (such as servers 23 and 24) on a network or
10 resources with aliases on a network can be stored and used for rewriting a link on the gateway apparatus.

[0044]

For example, if equivalent resources are on servers 23 and 24, the link may be rewritten in such a
15 manner that the load is appropriately distributed. If a resource equivalent to a resource on the external network 12 is on the internal network, a link may be rewritten so as to point the internal resource.

[0045]

20 Thus, users can efficiently access resources. A specific example of server access according to the present invention will be described below. A URL in the WWW will be described first. A URL (Universal Resource Locator) indicates a location of information.
25 A URL consists three portions. An exemplary URL is shown below.

[0046]

`http://www.is.university.ac.jp/welcome.html`

The first portion preceding the colon ("http" in this example) indicates the protocol to be used for accessing the server. In this example, the first
5 portion indicates HTTP (Hyper Text Transfer Protocol), which is the protocol for the WWW.

[0047]

The next portion between "://" and "/" indicates the name of the server. In this case, it is indicated
10 that the specified information is on the machine at "www.is.university.ac.jp". (It should be noted that this portion may include information indicating the port of the server to be accessed.) The remaining portion indicates the path to the information at the
15 server. In this example, it is "welcome.html".

[0048]

Figure 7 is a diagram for explaining a specific example of server access, showing an example of a WWW gateway. In this example, a network 11 internal to an
20 organization (company) includes a computer (client) 14, a gateway apparatus 1 machine directly connected to an external network 12 (external to the company), and the internal and external networks are interconnected through a router 15, which allows HTTP communications
25 to pass through it. Here, the gateway apparatus 1 machine is provisionally given the name of

"www.out.companyco.jp". HTTP servers 25, 26 and an FTP server 27 are provided on the external network 12.

[0049]

Assume that a user 13 wants to a Web page of the
5 information science department of a university having
the URL "http://www.is.university.ac.jp/welcome.html".
The user 13 first specifies on a client 14 the
following URL, instead of the ordinary URL.

[0050]

10 http://www-
out.company.co.jp/http://www.is.university.ac.jp/welcom
e.html

The client 14 interprets the URL and accesses the
gateway apparatus 1 having the machine name "www-
15 out.company.co.jp" by using HTTP. The router is set so
as to allow clients on the internal network to access a
particular machine on the external network by using a
certain protocol. The router 15 in this example is set
so as to allow HTTP communication to pass through it.
20 Accordingly, the client 14 can reach the gateway
apparatus 1 machine. The client 14 indicates the path
"http://www.is.university.ac.jp/welcome.html" to the
gateway apparatus 1 machine.

[0051]

25 The gateway apparatus 1 machine uses the given
path to attempt to access the server 25 (with the
server name of "www.is.university.ac.jp"). Because the

gateway apparatus 1 machine is directly connected to the external network 12, it can successfully access such server machines. Then, the gateway apparatus 1 obtains the following information.

5 [0052]

<HTML>

<HEAD>

<TITLE>

Welcome Message (ABC Univ--Dept Info Sci)

10 </TITLE>

</HEAD>

<BODY>

<H1>

Welcome to ABC University <p>--Department of
15 Information Science.

</H1>

Welcome to our WWW server!---This is under
development, though.

<P>

20 This WWW server is run by Department of
Information Science,

ABC University (somewhere-cho, ABC,

Japan),

25 which is a new department
established in 1990.

We have a collection of images on the

Earth's environment (in preparation) and

weather information.

We also serve

5

GMS (Himawari) images

for Chugoku/Shikoku area.

<P>

</BODY>

10 </HTML>

Here, <HTML> indicates the start of the document
written in HTML (Hyper Text Markup Language) and

</HTML> indicates the end of the document. <HEAD>

indicates the start of the header of the document.

15 This header may be a title name or author name. Here,
the title name is written. </HEAD> indicates the end

of the header. <TITLE> indicates the start of the
title. </TITLE> indicates the end of the title.

<BODY> indicates the body of the document and </BODY>

20 indicates the end of the document. <H1> indicates the
start of a level 1 section and </H1> indicates the end
of the level 1 section. <P> indicates the start of a
paragraph; an indication of the end of a paragraph is
not necessary.

25 [0053]

The hypertext changing device 4 of the gateway
apparatus 1 modifies the information given above by

changing the information " ... ",
which is a link, according to the obtained information
and information on the page being accessed, as follows.

[0054]

```

5      <HTML>

      <HEAD>

      <TITLE>
Welcome Message (ABC Univ--Dept Info Sci )
      </TITLE>
10     </HEAD>

      <BODY>

      <H1>
Welcome to ABC University <p>--Department of
Information Science.
15     </H1>

Welcome to our WWW server!---This is under
development, though.

      <P>

This WWW server is run by Department of
20 Information Science,

ABC University (somewhere-cho, ABC,

      <A HREF="http://www-
out.company.co.jp/http://www.xyz.jp/japan/index.html">J
apan</A>),
25     which is a new department
established in 1990.

We have a collection of images on the

```


Earth's environment (in preparation) and

```
<A HREF="http://www-
out.company.co.jp/http://www.is.university.ac.jp/FTP/im
ages/sat/">
```

5 weather information.

We also serve

```
<A HREF="http://www-
out.company.co.jp/http://www.is.university.ac.jp/FTP/im
ages/sat/gms.polar/">
```

10 GMS (Himawari) images
for Chugoku/Shikoku area.

```
<P>
</BODY>
</HTML>
```

15 The information thus modified is provided from the
gateway apparatus 1 to the client 14. The client 14
displays the information to the user 13 as shown in
Figure 8. It should be noted that the information
displayed to the user 13 is identical whether the

20 information is obtained directly from the server or
indirectly through the gateway, because the changed
link information is hidden from the user 13. That is,
the two hypertexts given above are identical in
appearance when displayed on the client 14.

25 [0055]

When the user 13 clicks the first link "Japan"
with a mouse, for example, the URL "http://www-

out.company.co.jp/http://www.xyz.jp/japan/index.html" is specified on the client 14 and the exactly the same cycle described above is repeated.

[0056]

- 5 If a non-HTTP server (for example FTP or GOPHER server) external server to the company is to be accessed, a similar change is made. For example, the URL of information at an FTP server,

ftp://ftp.uvw.edu/gutenberg/etext93/pimil10.txt

- 10 may be changed as follows:

[0057]

http://www-

out.company.co.jp/ftp://ftp.uvw.edu/gutenberg/etex93/pimil10.txt

- 15 Thus, access from the client 14 internal to the company to the external gateway apparatus 1 machine is made by using HTTP. Access from the external gateway apparatus 1 to an external server 27 is made by using FTP. The gateway apparatus 1 machine converts the
20 information obtained by using FTP into hypertext and returns the information to the client by using HTTP. In the hypertext conversion, the link is changed of course so that the gateway apparatus 1 is re-accessed.

[0058]

- 25 If the user 13 accesses the external server 27 through the gateway apparatus 1 and the server 27 has a file such as "Mac · Unix · X11", the hypertext

generating device 5 in the gateway apparatus 1 converts the file into a hypertext and returns the information to the client 14 by using HTTP.

[0059]

5 In this case, the client 14 will present the link "Mac · Unix · X11" to the user 13. Of course, the link is written so that the gateway apparatus 1 is re-accessed.

[0060]

10 [Advantages of the Invention]

 According to the present invention, an ordinary hypertext-based client can be used on a computer on a network internal to an organization to directly access a resource on an external network without scarifying
15 security as has been described, and accordingly the working efficiency can be improved.

[Brief Description of the Drawings]

[Figure 1]

 Figure 1 is a diagram for explaining the principle
20 of the present invention.

[Figure 2]

 Figure 2 is a block diagram showing a configuration of a gateway apparatus in an embodiment.

[Figure 3]

25 Figure 3 is a diagram for explaining a hypertext changing device in the embodiment.

[Figure 4]

Figure 4 is a diagram illustrating a hypertext generating device in the embodiment.

[Figure 5]

Figure 5 is a flowchart illustrating the
5 embodiment.

[Figure 6]

Figure 6 is a diagram for explaining server access in the embodiment.

[Figure 7]

10 Figure 7 is a diagram for explaining a specific example of server access in the embodiment.

[Figure 8]

Figure 8 is a diagram showing a display screen in the embodiment.

15 [Figure 9]

Figure 9 is a diagram illustrating a first example of the conventional art.

[Figure 10]

Figure 10 is a diagram illustrating a second
20 example of the conventional art.

[Description of Symbols]

- 1 Gateway apparatus
- 2 Link analyzing device
- 3 Various network services access control device
- 25 4 Hypertext changing device
- 5 Hypertext generating device

[Figure 1]

Diagram for explaining principle of the invention

- 2 Link analyzing device
- 3 Various network services access control device
- 5 5 Hypertext generating device
- 4 Hypertext changing device
- #1 Link information
- #2 Access information
- #3 Obtained information
- 10 #4 Hypertext
- #5 Gateway apparatus

[Figure 2]

Diagram of configuration of gateway apparatus

- 15 7 Network controller
- 6 Access monitor and control device
- 2 Link analyzing device
- 3 Various network services access control device
- 5 Hypertext generating device
- 20 4 Hypertext changing device
- #1 Network
- #2 Information from server
- #3 Control signal
- #4 Link information
- 25 #5 Access information
- #6 Hypertext
- #7 Obtained information

#8 Gateway apparatus

[Figure 3]

Diagram for explaining hypertext changing device

- 41 Link replacing unit
- 5 42 Link changing unit
- 4 Hypertext changing device
- #1 Hypertext
- #2 Extracted link
- #3 Changed link
- 10 #4 Hypertext changing device

[Figure 4]

Diagram for explaining hypertext generating device

- 51 Hypertext generating unit
- 15 52 Link setting unit
- 5 Hypertext generating device
- #1 Obtained information
- #2 Hypertext
- #3 Control signal
- 20 #4 Link

[Figure 5]

Flowchart in embodiment

- S1 Access monitor and control device determines
- 25 whether there is access from client
- S2 Receives link information and provides it to link
- analyzing device

- S3 Link analyzing device extract access information
and provides it to network services access control
device
- S4 Various network services access control device
5 obtains specified information based on access
information
- S5 Is obtained information hypertext?
- S7 Provides obtained information to hypertext
generating device to change ordinarily generated
10 link information by processing
- S6 Provides obtained information (hypertext) to
hypertext changing device to change link by
processing
- S8 Provides hypertext to access monitor and control
15 device
- S9 Access monitor and control device returns
hypertext to client

[Figure 6]

- 20 Diagram for explaining server access in embodiment
- 12 External network
- 20 to 24 Server
- 1a, 1b, 1c Gateway
- 15 Router allowing only limited protocols to pass
25 through it
- 11 Internal network
- 14 Computer

13 User

[Figure 7]

Diagram for explaining example of server access

5 25 to 27 Server

[Figure 8]

Diagram for explaining display screen

10 [Figure 9]

Diagram for explaining first example of conventional
art

12 External network

11 Internal network

15 14, 16 Computer

15 Router allowing only limited protocols to pass
through it

13 User

20 [Figure 10]

Diagram for explaining second example of conventional
art

12 External network

11 Internal network to organization

25 18 ZZZ server

14, 16 Computer

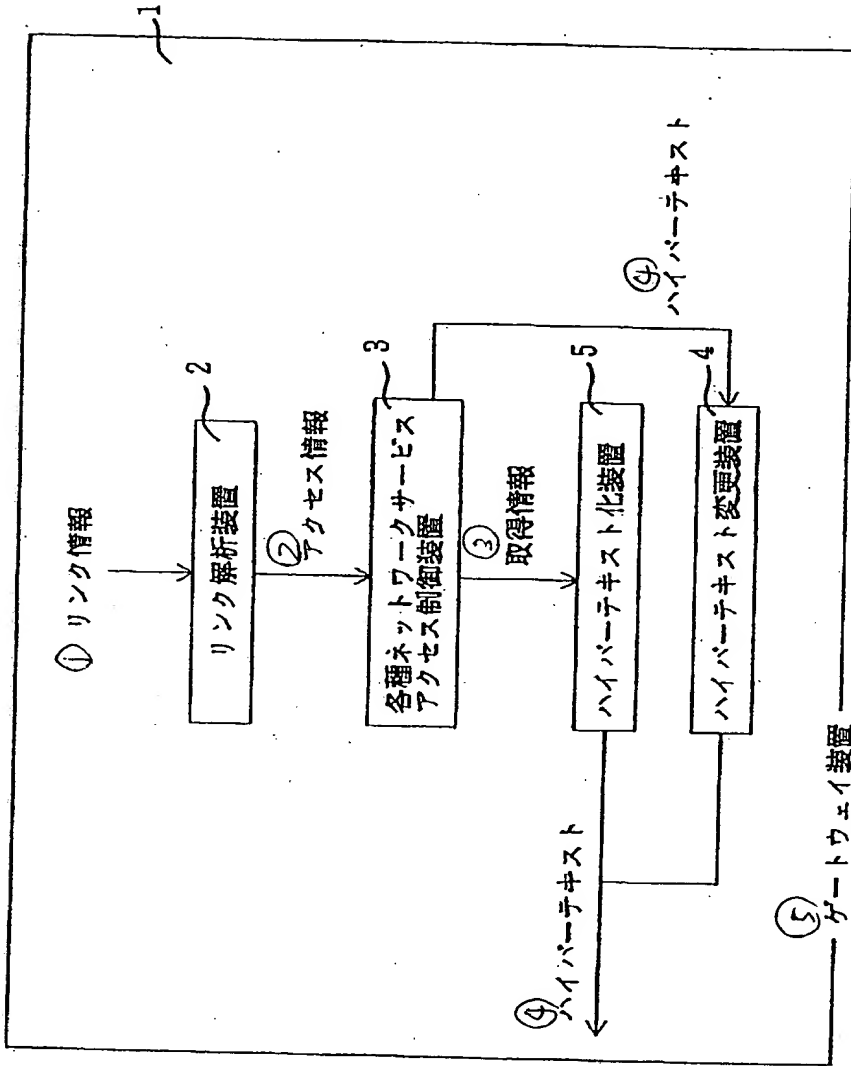
15 Router allowing only limited protocols to pass
through it

17 Special client (using ZZZ)

13 User

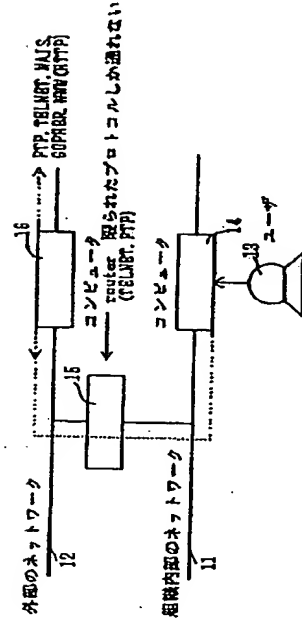
【図1】 FIG. 1

本発明の原理説明図



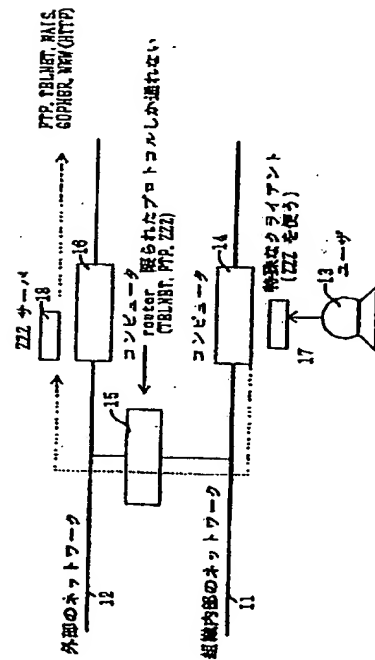
【図9】 FIG. 9

従来例 1 の説明図



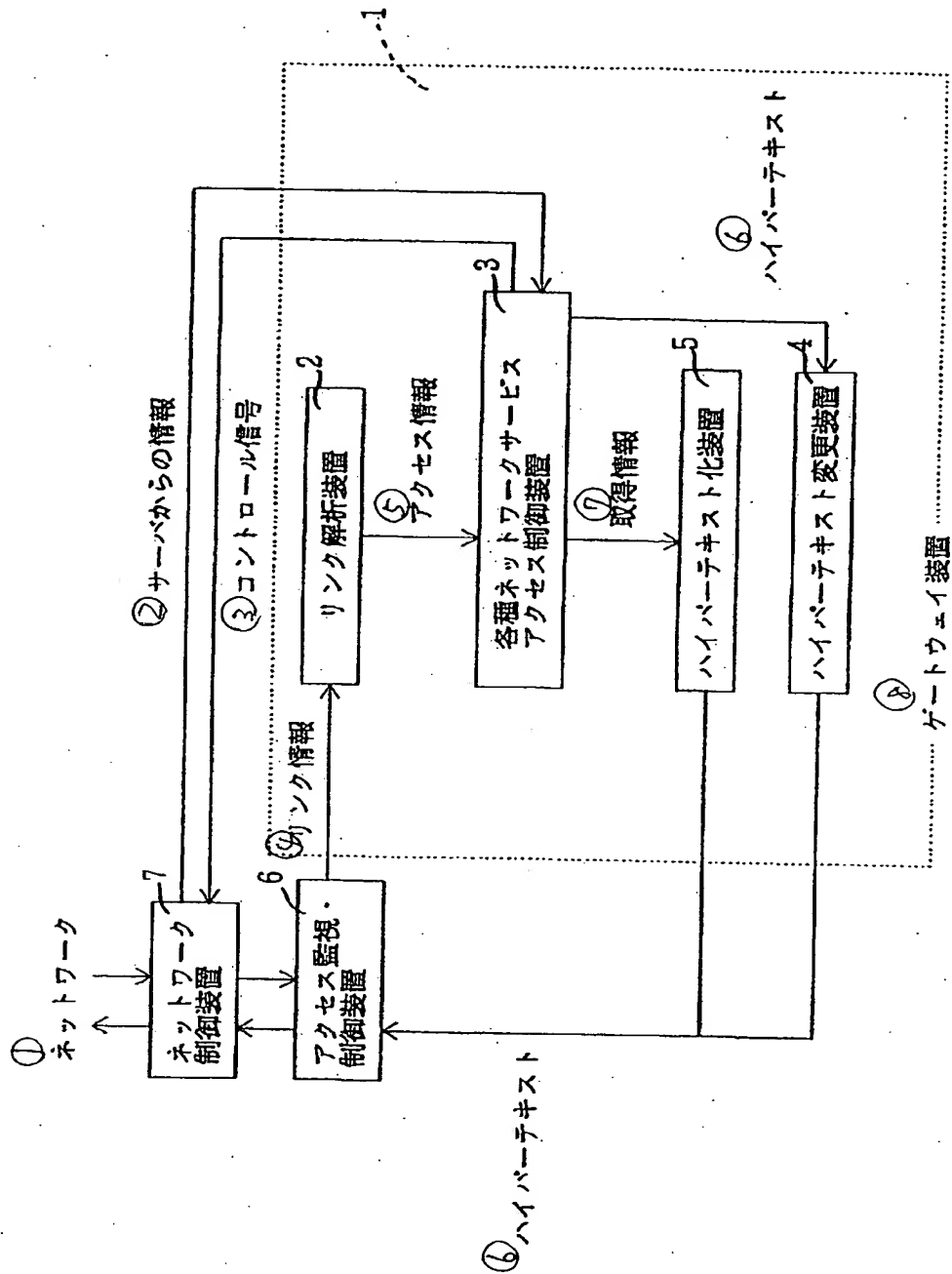
【図10】 FIG. 10

従来例 2 の説明図



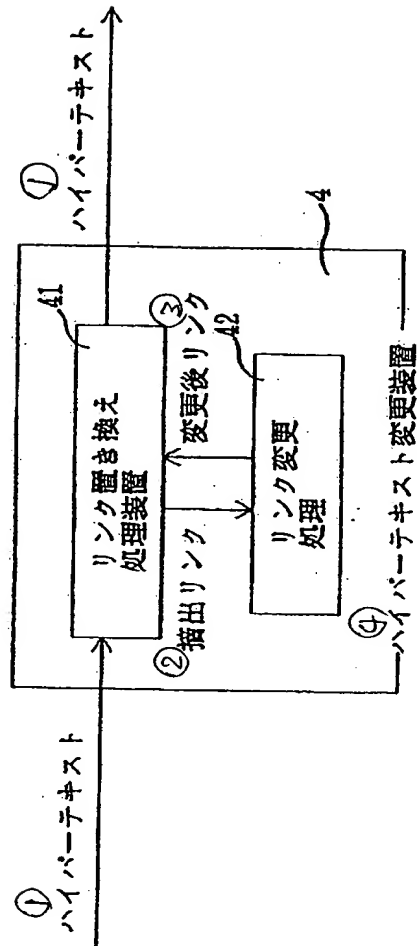
【図2】

ゲートウェイ装置の構成図



【図3】 FIG. 3

ハイパーテキスト変更装置の説明図

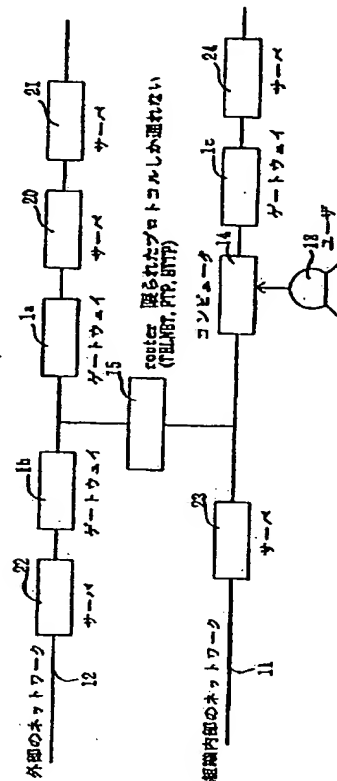
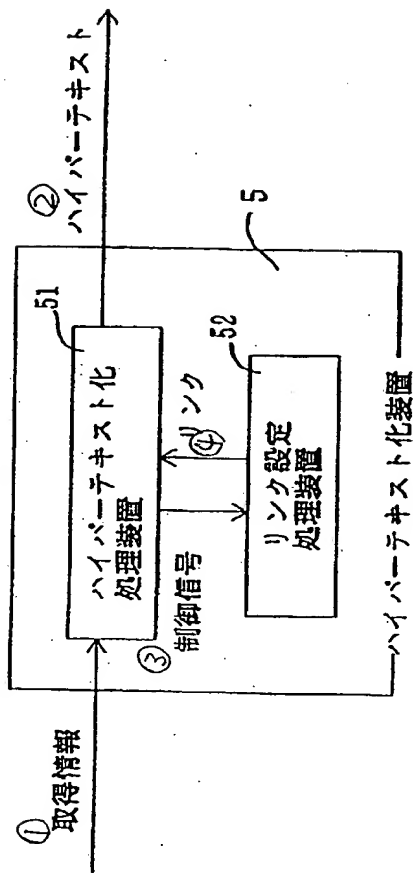


【図4】 FIG. 4

【図6】 FIG. 6

ハイパーテキスト化装置の説明図

実施例におけるサーバアクセス説明図



特開平8-44643

(43) 公開日 平成8年(1996)2月16日

(51) Int. Cl. ^a	識別記号	庁内整理番号	F I	技術表示箇所
G06F 13/00	353	C 7368-5E		
	355	7368-5E		
12/00	547	H 7623-5B		

審査請求 未請求 請求項の数 9 O L (全14頁)

(21) 出願番号	特願平6-175125	(71) 出願人	000005223 富士通株式会社 神奈川県川崎市中原区上小田中1015番地
(22) 出願日	平成6年(1994)7月27日	(72) 発明者	益岡 竜介 神奈川県川崎市中原区上小田中1015番地 富士通株式会社内
		(72) 発明者	岡田 浩之 神奈川県川崎市中原区上小田中1015番地 富士通株式会社内
		(72) 発明者	末松 伸朗 神奈川県川崎市中原区上小田中1015番地 富士通株式会社内
		(74) 代理人	弁理士 山谷 皓榮 (外1名)

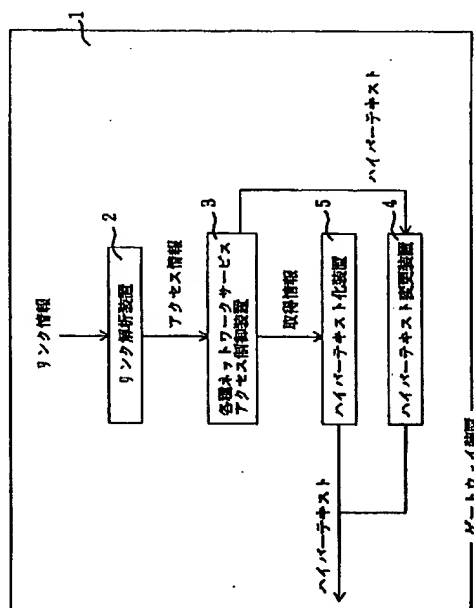
(54) 【発明の名称】 ゲートウェイ装置

(57) 【要約】

【目的】 ハイパーテキストを用いることにより、特別なクライアントを用いずに、しかもセキュリティを犠牲にせず、ユーザに対して透明なままで外部のデータベースにアクセス可能とすることを目的とする。

【構成】 ハイパーテキストのリンクの置き換えをするリンク置き換え処理装置と、リンクの変更をするリンク変更処理装置とをハイパーテキスト変更装置4に備え、リンク置き換え処理装置がハイパーテキストを受け取ると、リンク変更処理装置でリンク情報を特定の処理手段に従って変更した後、リンク置き換え処理装置がリンク情報変更後のハイパーテキストを出力するようにする。

本発明の原理説明図



【特許請求の範囲】

【請求項 1】 ハイパーテキストのリンクの置き換えをするリンク置き換え処理手段と、
リンクの変更をするリンク変更処理手段とをハイパーテキスト変更装置に備え、

リンク置き換え処理手段がハイパーテキストを受け取ると、リンク変更処理手段でハイパーテキスト中のリンク情報を特定の処理手段に従って変更した後、前記リンク置き換え処理手段が前記リンク情報変更後のハイパーテキストを出力するようにするハイパーテキスト変更装置を備えることを特徴としたゲートウェイ装置。

【請求項 2】 ハイパーテキスト化するハイパーテキスト化処理手段と、

リンクを生成するリンク設定処理手段とをハイパーテキスト化装置に備え、

ハイパーテキスト化処理手段で取得情報をハイパーテキスト化し、

リンク設定処理手段でリンク情報を特定の処理手段に従って変更した後、

前記ハイパーテキスト化処理手段が前記リンク情報変更後のハイパーテキストを出力するハイパーテキスト化装置を備えることを特徴としたゲートウェイ装置。

【請求項 3】 前記リンク情報を変更する特定の処理手段として、再び同じゲートウェイにアクセスする情報を加える手段を設けることを特徴とした請求項 1 又は 2 記載のゲートウェイ装置。

【請求項 4】 前記リンク情報を変更する特定の処理手段として、再び同じゲートウェイ或いは他のゲートウェイにアクセスする情報を加える手段を設けることを特徴とした請求項 1 又は 2 記載のゲートウェイ装置。

【請求項 5】 前記リンク情報を変更する特定の処理手段として、他のサーバにアクセスする情報を設ける手段を備えることを特徴とした請求項 1 又は 2 記載のゲートウェイ装置。

【請求項 6】 リンク情報を受け取り、リンク情報を解析するリンク解析装置と、

該リンク解析装置からのアクセス情報をもとに、サーバにアクセスし、情報を取得する各種ネットワークサービスアクセス制御装置と、

前記取得情報がハイパーテキストの場合ハイパーテキストのリンク情報を特定の処理手段に従って変更するハイパーテキスト変更装置と、

前記取得情報がハイパーテキストでない場合ハイパーテキスト化すると共にリンク情報を特定の処理手段に従って変更するハイパーテキスト化装置とを備えることを特徴としたゲートウェイ装置。

【請求項 7】 前記リンク情報を変更する特定の処理手段として、再び同じゲートウェイにアクセスする情報を加える手段を設けることを特徴とした請求項 6 記載のゲ

ートウェイ装置。

【請求項 8】 前記リンク情報を変更する特定の処理手段として、再び同じゲートウェイ或いは他のゲートウェイにアクセスする情報を加える手段を設けることを特徴とした請求項 6 記載のゲートウェイ装置。

【請求項 9】 前記リンク情報を変更する特定の処理手段として、他のサーバにアクセスする情報を設ける手段を備えることを特徴とした請求項 6 記載のゲートウェイ装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明はハイパーテキスト中のリンクを変更する、あるいはハイパーテキストによるゲートウェイを実現する装置に関する。

【0002】 近年、ネットワーク上に分散したデータベースおよび、それらにアクセスするためのクライアントが各種出てきている。それらをサポートするネットワークのプロトコルには、ローカルファイルシステム (LOCAL FILE SYSTEM)、エフティピ (FTP)、インタネットニュース (INTERNET NEWS)、テルネット (TELNET)、ウェイズ (WAIS)、ゴファ (GOPHER)、ワールドワイドウェブ (WWW: World Wide Web) の HTTP (Hyper Text Transfer Protocol) などがある。特に WWW では直接、或いはゲートウェイを使って他のプロトコルを使うサーバにアクセスして、それらの結果を最終的にハイパーテキストにしてユーザに表示している。

【0003】 さてこのようにいろいろな情報が簡単に手に入るが、会社などの情報のセキュリティを守る必要のある組織では外部とのアクセスを制限しているところが多い。しかし一方でネットワーク上の各種データベースが充実するにつれ、それらのデータに簡単にアクセスすることが要求されている。

【0004】 このため、必要なデータベースのセキュリティを守りながら、ユーザに対して外部のデータベースに対しても内部のデータベースにアクセスするのと同様のアクセス、即ち透明なアクセスを実現することが要望されている。

【0005】

【従来の技術】 まず、ここで使用する言葉の定義をする。サーバ (server) は、データベースを持ち、特定のプロトコルを使ってアクセスしてきたクライアントに対して情報を提供するものである。

【0006】 クライアント (client) は、特定のプロトコルを使ってサーバが持つ情報を取ってくるものであり、通常ソフトウェアで実現されているものである。プロトコル (protocol) は、コンピュータとコンピュータがある目的 (例えばファイルをやりとりするなど) を持って通信しあう際の取り決めである。

【0007】 ハイパーテキスト (hypertext) は、情報

を提示するための一方法であり、文書中のいくつかの言葉がリンクになっており、それらの言葉が選ばれるとそのリンクが指す先の文書が表示されるようになっている。そして、リンクの指す先の文書はハイパーテキスト、通常のテキスト、静止画、動画、音、その他何でも構わないものである。

【0008】リンク (link) は、言葉が指す文書にどうすればアクセスできるかを示した文字列のことであり、このリンクはハイパーテキストをフォーマットとして表示するクライアントでは通常ユーザから見えないように隠されている。例えば文字列に「どのプロトコルで、どこのマシンのどのファイルにアクセスする」といった情報が含まれているものである。

【0009】従来にも、組織の外部のネットワークに設けられたサーバに組織の外部のネットワークのコンピュータではなく、組織内部のコンピュータから直接組織外部のサーバにアクセスする方法があった。

【0010】この場合に組織のセキュリティを確保する方法は、通常次のようなものがある。組織の外部のネットワークと内部のネットワークをルータ (router) で接続する。そして、このルータではそこを通れるプロトコルの種類とその方向を制限し、それを防壁 (firewall) として組織内部のセキュリティを確保するものである。

【0011】図9、図10は、従来例の説明図であり、以下、図9の従来例1に基づいて説明する。図9において、組織内部のネットワーク11には、ユーザ13が使用するコンピュータ14が設けてある。組織の外部のネットワーク12には、コンピュータ16と各種のプロトコルであるFTP、TELNET、WAIS、GOPHER、HTTPをもつサーバ (図示せず) が接続されている。そして、組織内部のネットワーク11と外部のネットワーク12は、限られたプロトコル (TELNET、FTP) しか通れないルータ15を介して接続されている。

【0012】このような環境の下で外部にアクセスを確保する方法は、組織の外部のネットワーク上の何台かの (図では1台を示す) コンピュータ16に、組織内部から外部のネットワークに用意されたコンピュータ16にTELNET、FTPなどを使ってアクセスできるようにしておく。これにより組織内部のネットワーク上に置いてあるコンピュータ14を使ってユーザ13が外部にアクセスする必要がある場合には、まず、組織内部のマシンであるコンピュータ14から、例えばTELNETでルータ15を通して組織外部のネットワーク12に用意されたコンピュータ16に入り、次に、その他の組織外部のマシンにコンピュータ16で変更された各種のプロトコルでアクセスして情報を得るようにしていた。

【0013】また、組織内部のセキュリティを確保しながら組織外部にアクセスを確保する他の方法として図10の従来例2があった。以下、図10に基づいて説明す

る。図10中、図9と同じものは同じ符号で示す。

【0014】図10において、新たにZZZというプロトコル (ZZZは仮の名前である) がルータ15を通れるようにする。そして、ルータ15を通れない通常のプロトコル例えばGOPHER、HTTPなどを使うクライアントであるコンピュータ14を変更して、ZZZのプロトコルを使う特殊なクライアント17とする。また、組織の外部のネットワーク12にゲートウェイ装置であるZZZのサーバ18を設ける。

【0015】組織内部のネットワーク11からユーザ13が外部にアクセスする必要が生じた場合、まず、ZZZのプロトコルを使って、ルータ15を通り外部のネットワーク12上のコンピュータ16上で走っているZZZサーバにアクセスする。次に、ZZZサーバ18がクライアント17の代わりに外部のネットワーク12上にある例えばGOPHER、HTTPなどのサーバにアクセスし、クライアント17にその情報を返していた。

【0016】

【発明が解決しようとする課題】上記従来のものにおいては、次のような課題があった。従来例1のように、外部のネットワーク12上のコンピュータ16を使う方法は、1度コンピュータ16の内部に入る例えばログインの手続などのため非常に手間がかかる。また、例えば自分の使うコンピュータ14からグラフィカル表示をするウィンドウ対応のクライアントを使おうと思ってもルータ15がTELNET等のキャラクタベース (character base) のプロトコルしか通さないので使用できないなど、組織内部のネットワーク上にある自分の使うコンピュータ14から、直接決まったプロトコルを使って、外部のサーバと通信する必要がある場合、一般のクライアントを使えないという欠点があった。

【0017】また、従来例2のように、プロトコルZZZのような特殊なクライアント17を使う方法は、自分の使うコンピュータからクライアントが使えるが、使おうとするクライアントはそのまま使えず、使いたい通常のクライアントを、特別なプロトコルであるZZZを使って通信するような特別なクライアント17に変更する必要があった。

【0018】本発明は、ハイパーテキストを用いることにより特別なクライアントを用いずに、セキュリティを犠牲にせず、ユーザに対して透明なままで、外部のデータベースにアクセスすることを目的とする。

【0019】

【課題を解決するための手段】本発明は、上記課題を解決するため次のように構成した。図1は、本発明の原理説明図であり、図1において、ゲートウェイ装置1は、リンク情報を解析するリンク解析装置2、各種ネットワークサーバにアクセスして指定された情報を取得する各種ネットワークサービスアクセス制御装置3、取得情報のハイパーテキストを変更するハイパーテキスト変

更装置4、取得情報をハイパーテキスト化するハイパーテキスト化装置5が設けてある。

【0020】

【作用】上記構成に基づく本発明の作用を、図1に基づいて説明する。まず、リンクの情報をリンク解析装置2が受け取る。リンク解析装置2は、リンクを解析し、アクセスするための情報であるアクセス情報に変更して各種ネットワークサービスアクセス制御装置3に渡す。各種ネットワークサービスアクセス制御装置3は、このアクセス情報を元に各種ネットワークサーバにアクセスし、アクセス情報に指定された情報を取得する。この取得した情報である取得情報が、ハイパーテキストである場合にはハイパーテキスト変更装置4に渡す。ハイパーテキスト変更装置4は、取得情報の中のリンク情報が与えられた処理方法に従って、このゲートウェイ装置1あるいはその他のゲートウェイ装置あるいはその他のサーバにアクセスするように書き換え(変更)られたハイパーテキストを出力するものである。

【0021】前記各種ネットワークサービスアクセス制御装置3の取得情報がハイパーテキストでない場合には、その取得情報をハイパーテキスト化装置5に渡す。これにより、ハイパーテキスト化装置5は、取得情報の中のリンク情報がこのゲートウェイ装置1あるいはその他のゲートウェイ装置あるいはその他のサーバにアクセスするように設定したハイパーテキストを出力することになる。

【0022】このような、ゲートウェイ装置1を外部のネットワーク12上に設けると組織内部のネットワーク上のコンピュータから通常のハイパーテキストのクライアントを使って、しかもセキュリティを犠牲にすることなく、外部のネットワーク上にあるリソース(資源)にアクセスできるようになる。

【0023】

【実施例】本発明の実施例を図2～図8に基づいて説明する。図中、図1と同一のものは同一の符号で示してある。

【0024】図2は、本発明の実施例におけるゲートウェイ装置の構成図であり、ネットワーク制御装置7は、ネットワークを使って行う通信の制御をするものである。アクセス監視・制御装置6は、ネットワーク制御装置7を監視し、アクセスがあったかを監視している。

【0025】アクセス監視・制御装置6は、他のクライアントからアクセスがあると、そのクライアントから与えられたリンク情報をゲートウェイ装置1に渡す。ゲートウェイ装置1は、通常とは異なるリンクを持ったハイパーテキストをアクセス監視・制御装置6に返す。これにより、アクセス監視・制御装置6は、ネットワーク制御装置7を制御してアクセスしてきたクライアントにそのハイパーテキストを返すものである。

【0026】この際、例えばハイパーテキストのリンク

に再びこのゲートウェイ装置1をアクセスしてから、そのゲートウェイ装置1からもとのリンクの指していた先にアクセスするように書いておけば、クライアントを使うユーザがこのリンクを選択すると自動的にこのゲートウェイに再びアクセスするようになる。

【0027】図3は、ゲートウェイ装置1のハイパーテキスト変更装置の説明図である。ハイパーテキスト変更装置4には、リンク置き換え処理装置41とリンク変更処理装置42が設けてある。

【0028】以下、このハイパーテキスト変更装置4がハイパーテキストを入力として受け取った時の説明をする。まず、リンク置き換え処理装置41がハイパーテキストを受け取る。リンク置き換え処理装置41は、ハイパーテキストからリンクを抽出し、それをリンク変更処理装置42に渡す。リンク変更処理装置42は、予め与えられた処理方法に従ってリンクを変換し(例えば、このゲートウェイ装置1にアクセスするように変換する)、変更後リンクをリンク置き換え処理装置41に与える。

【0029】リンク置き換え処理装置41は、ハイパーテキスト中の元の抽出されたリンクを変更後のリンクに置き換え、最終的に得られたハイパーテキストを出力する。図4は、ゲートウェイ装置のハイパーテキスト化装置の説明図である。ハイパーテキスト化装置5には、ハイパーテキスト化処理装置51とリンク設定処理装置52が設けてある。

【0030】以下、ハイパーテキスト化装置5が取得情報を入力として受け取った時の説明をする。ハイパーテキスト化処理装置51が例えば、FTP、GOPHERなどの形態の情報であるいろいろな形態の取得情報を受け取る。そして、リンク以外の部分は通常の方法でハイパーテキスト化する。リンクの部分の生成する段になると、ハイパーテキスト化処理装置51は、リンク設定処理装置52に必要な制御信号(情報)を与える。

【0031】リンク設定処理装置52は、予め与えられた処理方法に従ってリンクを生成し、ハイパーテキスト化処理装置51に与える。これによりハイパーテキスト化処理装置51は、そのリンクを通常の方法でのハイパーテキストに統合し、最終的に得られたハイパーテキストを出力する。

【0032】例えば、上記取得情報が、
(プロトコルA+サーバA+付加情報)

であるとすると、このリンク設定処理装置52で、このゲートウェイ装置1にアクセスするように書き換える場合は、

プロトコル+このゲートウェイ+ (プロトコルA+サーバA+付加情報)

のようにリンク情報を付加する。

【0033】この付加したリンク情報は、クライアントのユーザからは隠されているのでユーザには見えない。

従って、ユーザは、外部のネットワーク上でクライアントを動かしているのと全く同様に、組織内部のネットワークから外部のネットワークの各種サーバに自由にアクセスできるように見える。

【0034】図5は、本発明の実施例のフローチャートである。以下、図5のフローチャートに基づいてゲートウェイ装置1の動作を説明する。S1～S9は処理番号を示す。

【0035】まず、アクセス監視・制御装置6がクライアントからアクセスがあるかを調べる(S1)。クライアントからアクセスがあるとアクセス監視・制御装置6は、リンク情報を受け取りリンク解析装置2に渡す(S2)。リンク解析装置2は、アクセス情報を取り出して各種ネットワークサービスアクセス制御装置3に渡す(S3)。各種ネットワークサービスアクセス制御装置3は、アクセス情報を元に指定された情報をネットワーク制御装置7を通して取得する(S4)。

【0036】各種ネットワークサービスアクセス制御装置3は、取得情報がハイパーテキストかどうかを判断する(S5)。この取得情報がハイパーテキストであれば(Yes)各種ネットワークサービスアクセス制御装置3は、ハイパーテキスト変更装置4に取得情報(ハイパーテキスト)を渡し、ハイパーテキスト変更装置4でリンクを予め与えられた処理に従って変更する(S6)。もし、処理番号S5で取得情報がハイパーテキストでなければ(No)各種ネットワークサービスアクセス制御装置3は、ハイパーテキスト化装置5に取得情報を渡し、ハイパーテキスト化装置5は、通常生成されるリンク情報を予め与えられた処理に従って変更してハイパーテキストを出力する(S7)。

【0037】前記処理番号S6、またはS7で処理されたハイパーテキストがアクセス監視・制御装置6に渡される(S8)。アクセス監視・制御装置6がハイパーテキストをネットワーク制御装置7を通してクライアントに返す(S9)。

【0038】図6は、実施例におけるサーバアクセス説明図である。以下、図6に基づいて説明する。図6において、外部のネットワーク12には、ゲートウェイ装置1a、1b、サーバ20～22が設けてあり、組織内部のネットワーク11には、ゲートウェイ装置1c、コンピュータ14、サーバ23、24が設けてある。ルータ15は、組織内部のネットワーク11と外部のネットワーク12を接続しており、例えば、TELNET、FTP、HTTP等の限られたプロトコルしか通れないものである。

【0039】ユーザ13がセキュリティを保ったまま組織内部のネットワーク11上にあるコンピュータ14から外部のサーバ20へアクセスするためには、外部のネットワーク12にゲートウェイ装置1aを置く。更にルータ15は、通常許しているプロトコル(例えば、TE

LN E T、FTP)に加えて、例えばハイパーテキストをやりとりするプロトコルであるHTTPのプロトコルを組織内部のネットワーク11の方から通ることを許すようにしておく。

【0040】これにより、一度このゲートウェイ装置1aを通じて外部のネットワーク上にあるサーバ20のリソースにアクセスすれば、アクセスした結果は全てハイパーテキストで返され、リンクは全て再びこのゲートウェイ装置1aにアクセスするように設定される。以後このアクセス過程を何度繰り返してもリンクがこのゲートウェイ装置1aにアクセスするように設定されているので、クライアントのユーザ13がリンクを選択するとこのゲートウェイ装置1aにまずアクセスするようになる。

【0041】また、外部のネットワーク12にこのようなゲートウェイ装置1aをいくつか設ける(例えばゲートウェイ装置1b)場合には、それらのゲートウェイ装置1a、1bを適当な方法で選択してリンクに書き込めば、それらのゲートウェイ装置1a、1bの間で負荷分散することも可能となる。

【0042】例えば、元のリンクの指す先を解析してその指す先に近いゲートウェイ装置を選択する。ゲートウェイ装置1aの負荷によって他のゲートウェイ装置1bに回すようにする。適当に(例えば乱数により)ゲートウェイを選択する。更に、ゲートウェイ間の通信によって負荷の少ないゲートウェイ装置に回す等の方法で行う。

【0043】更に、セキュリティを確保するためだけのゲートウェイ装置でなく、次のようにしても実施可能である。同じネットワーク上のリソースがいくつかの場所にある(例えばサーバ23、24)場合や、ネットワーク上のリソースに別名がついている場合など、それらの情報を貯めておき、ゲートウェイ装置でリンクを書き換える際にそれらを使って書き換えることもできる。

【0044】例えば、同等のネットワーク上のリソースがサーバ23、24にある場合は、適当に負荷を分散するように書き換える。また、外部のネットワーク12上のリソースと同等のリソースが内部のネットワークにある場合には、リンクを内部のリソースを指すように書き換えてしまうこともできる。

【0045】このように、ユーザはリソースに効率のよいアクセスが可能となる。以下、本発明のサーバアクセスを具体例で説明する。まず、WWWにおけるURLを説明する。URL(Universal Resource Locator)とは、情報のありかを示すものである。これは三つの部分からなっており、以下にURLの具体例を示す。

【0046】

<http://www.is.university.ac.jp/welcome.html>

最初の「:」までの部分(この場合は「http」)はそのサーバへのアクセス方法を示す。この場合はWWWのプ

ロトコルであるHTTP (Hyper Text Transfer Protocol) である。

【0047】次の「:/」と「/」の間はサーバの名前を示す。この場合は指定された情報が「www.is.university.ac.jp」というマシンにあることを示している

(なお、この部分でさらにサーバのどのポートにアクセスすればよいのかの情報が与えられる時もある)。残りの部分はそのサーバでの情報のパス (path) が示される。この例の場合では「welcome.html」である。

【0048】図7は、サーバアクセスの具体例の説明図であり、WWWのゲートウェイの例を示す。この例では、組織内部 (社内) のネットワーク11にコンピュータ (クライアント) 14があり、外部 (社外) のネット

http://www-out.company.co.jp/http://www.is.university.ac.jp/welcome.html

クライアント14は、このURLを解釈し、HTTPでマシン名「www-out.company.co.jp」のゲートウェイ装置1にアクセスする。ルータは、社内のネットワークから特定のプロトコルで社外のネットワークの特定のマシンにアクセスできるように設定されている。この場合のルータ15は、HTTPを通すように設定しているの

20

```
<HTML>
<HEAD>
<TITLE>
Welcome Message (ABC Univ--Dept Info Sci)
</TITLE>
</HEAD>
<BODY>
<H1>
Welcome to ABC University <p>--Department of Information Science.
</H1>
Welcome to our WWW server!--This is under development, though.
<P>
This WWW server is run by Department of Information Science,
ABC University (somewhere-cho, ABC,
<A HREF="http://www.xyz.jp/japan/index.html">Japan</A>),
which is a new department
established in 1990.
We have a collection of images on the
Earth's environment (in preparation) and
<A HREF="/FTP/images/sat/">
weather information</A>.
We also serve
<A HREF="/FTP/images/sat/gms.polar/">
GMS (Himawari) images </A>
for Chugoku/Shikoku area.
<P>
```

ワーク12に直接つながったゲートウェイ装置1のマシンがあり、社外と社内のネットワークはHTTPを通すルータ15でつながっている。このゲートウェイ装置1のマシンの名前を仮に「www.out.company.co.jp」とし、社外のネットワーク12にはHTTPのサーバ25、26とFTPのサーバ27が設けてある。

【0049】最初にユーザ13はURLとして「http://www.is.university.ac.jp/welcome.html」をもつある大学情報科学科のホームページにアクセスしたいと思ったとする。この時ユーザ13は、まず通常のURLの代わりに次のようなURLをクライアント14に対して指定する。

【0050】

w.is.university.ac.jp/welcome.html」を示す。

【0051】ゲートウェイ装置1のマシンはその与えられたパスを元にHTTPでサーバ25 (サーバ名「www.is.university.ac.jp」) にアクセスしに行く。このゲートウェイ装置1は社外のネットワーク12に直接接続しているので問題なくそれらのマシンにアクセスできる。そして、このゲートウェイ装置1は情報として、以下のような情報をもらってくる。

【0052】

</BODY>

</HTML>

なお、上記<HTML>は、HTML (Hyper Text Markup Language) の形式で書かれた文書の始まりを示し、</HTML>は、その終りを示す。<HEAD>は、文書のヘッダの始まりを示し、このヘッダにはタイトル名やオーサ名などがあり、ここではタイトル名が書かれており、</HEAD>はヘッダの終りを示す。<TITLE>は、タイトルの始まりを示し、</TITLE>は、タイトルの終りを示す。<BODY>は、文書の本文を示し、</BODY>は、その終りを示す。<H1>は、セクションのレベル1の始まりを示し、</H

<HTML>

<HEAD>

<TITLE>

Welcome Message (ABC Univ--Dept Info Sci)

</TITLE>

</HEAD>

<BODY>

<H1>

Welcome to ABC University <p>--Department of Information Science.

</H1>

Welcome to our WWW server!---This is under development, though.

<P>

This WWW server is run by Department of Information Science,
ABC University (somewhere-cho, ABC,

Japan),

which is a new department
established in 1990.

We have a collection of images on the
Earth's environment (in preparation) and

weather information.

We also serve

GMS (Himawari) images
for Chugoku/Shikoku area.

<P>

</BODY>

</HTML>

このように変更された情報がゲートウェイ装置1からクライアント14に渡される。クライアント14側では、この情報を例えば図8のようにユーザ13に対して表示する。ここで注意して欲しいのは、書き換えられたリンクの情報はユーザ13から隠されるので、サーバから直接情報をもらった場合も、ゲートウェイを通して情報をももらった場合もユーザ13に対する表示は全く同じであ

1>は、その終りを示す。<P>は、パラグラフ（段落）の始まりを示しており、この終りは特に必要でない。

【0053】ゲートウェイ装置1は、もらってきた情報と今アクセスしているページの情報を元にリンクである「...」の情報をハイパーテキスト変更装置4で書き換えることにより、以下のように上の情報を変更する。

【0054】

ることである。即ち、上記二つのハイパーテキストをクライアント14は同じに表示することになる。

【0055】ここでユーザ13が例えば、一番最初のリンクである「Japan」をマウス等でクリックすれば、クライアント14に対してURLとして「http://www-out.company.co.jp/http://www.xyz.jp/japan/index.html」を指定したことになり、上と全く同じサイクルが繰

り返される。

【0056】社外のアクセス先がHTTP以外のサーバである場合（例えばFTP, GOPHER）にも同じように書き換えが行われる。例えば以下のようなFTPの

http://www-out.company.co.jp/ftp://ftp.uvw.edu/gutenberg/etext93/pimil

10.txt

このことにより、社内のクライアント14から社外のゲートウェイ装置1のマシンへはHTTPでアクセスが行われる。社外のゲートウェイ装置1のマシンからはFTPで社外のサーバ27へアクセスが行われる。ゲートウェイ装置1のマシンはFTPで得た情報をハイパーテキストに変換し、HTTPでクライアントにその情報を返す。当然上のハイパーテキストの変換では再びそのゲートウェイ装置1にアクセスが行われるようにリンクが書かれている。

【0058】また、ユーザ13がゲートウェイ装置1を通して社外のサーバ27にアクセスし、サーバ27に例えば「Mac・Unix・X11」等のファイルがあった場合、ゲートウェイ装置1は、ハイパーテキスト化装置5でハイパーテキストに変換して、HTTPでクライアント14にその情報を返す。

【0059】この場合、クライアント14は、ユーザ13に対して「Mac・Unix・X11」のリンク表示をすることになり、当然この場合も再びゲートウェイ装置1にアクセスが行われるようにリンクが書かれている。

【0060】

【発明の効果】以上説明したように、本発明によれば直接組織内部のネットワーク上のコンピュータから通常のハイパーテキストのクライアントを使って、セキュリティを犠牲にすることなく、外部のネットワーク上にある

サーバ27にある情報のURLの場合には

ftp://ftp.uvw.edu/gutenberg/etext93/pimil10.txt

次のように書き換えられる。

【0057】

リソースにアクセスできるようになり、作業の効率向上を行うことができる。

【図面の簡単な説明】

【図1】本発明の原理説明図である。

【図2】実施例におけるゲートウェイ装置の構成図である。

【図3】実施例におけるハイパーテキスト変更装置の説明図である。

【図4】実施例におけるハイパーテキスト化装置の説明図である。

【図5】実施例におけるフローチャートである。

【図6】実施例におけるサーバアクセス説明図である。

【図7】実施例におけるサーバアクセスの具体例の説明図である。

【図8】実施例における表示画面の説明図である。

【図9】従来例1の説明図である。

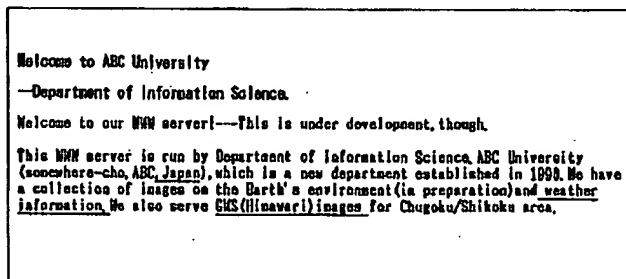
【図10】従来例2の説明図である。

【符号の説明】

- 1 ゲートウェイ装置
- 2 リンク解析装置
- 3 各種ネットワークサービスアクセス制御装置
- 4 ハイパーテキスト変更装置
- 5 ハイパーテキスト化装置

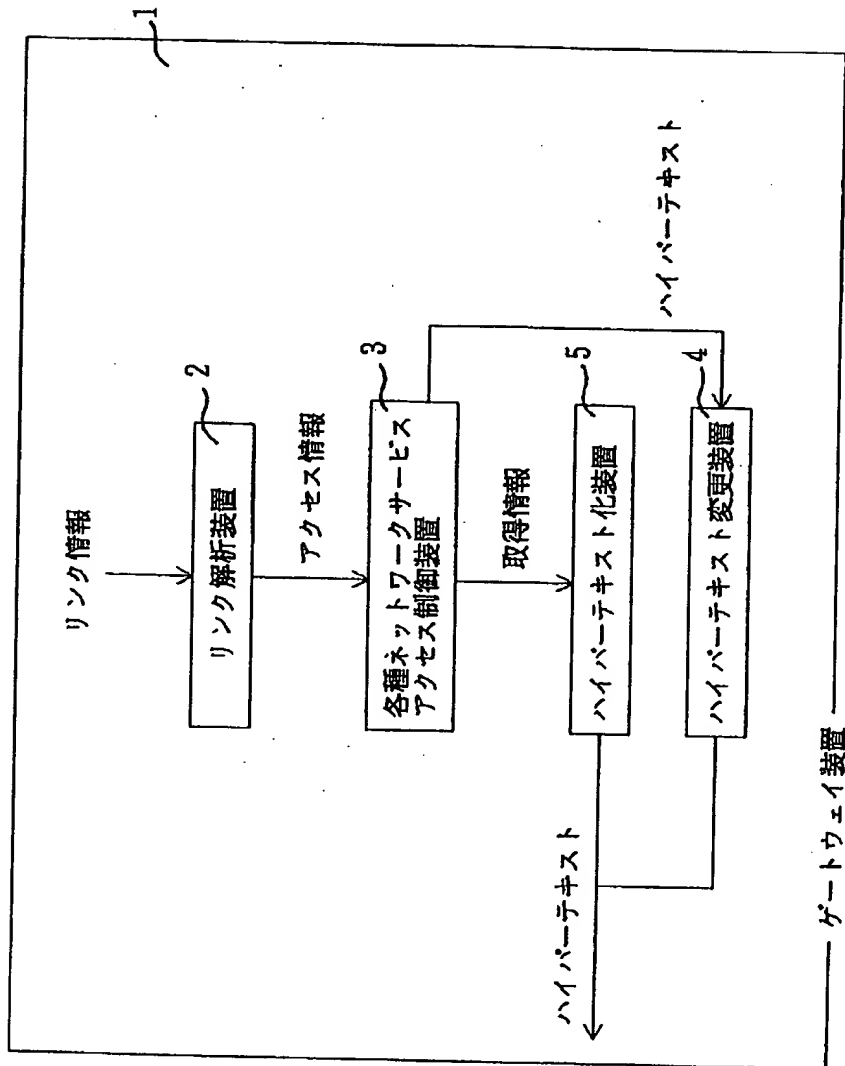
【図8】 *FIG. 8*

表示画面の説明図



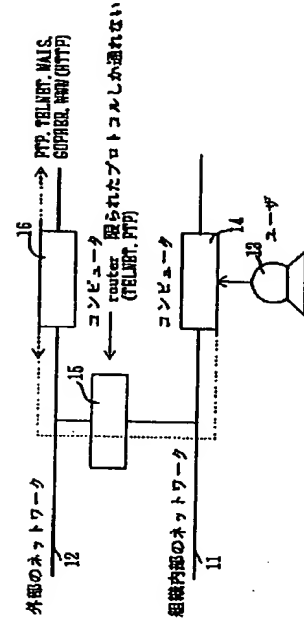
【図1】 FIG. 1

本発明の原理説明図



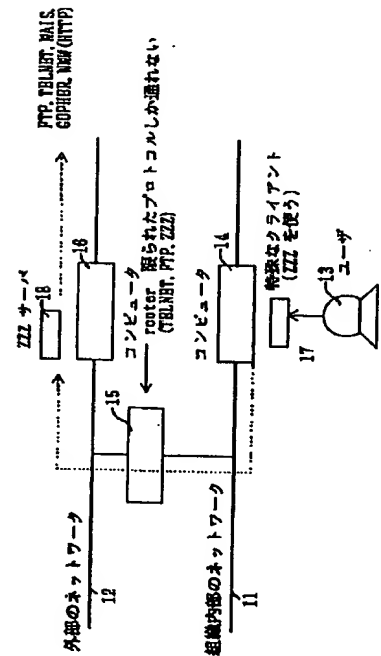
【図9】 FIG. 9

従来例1の説明図



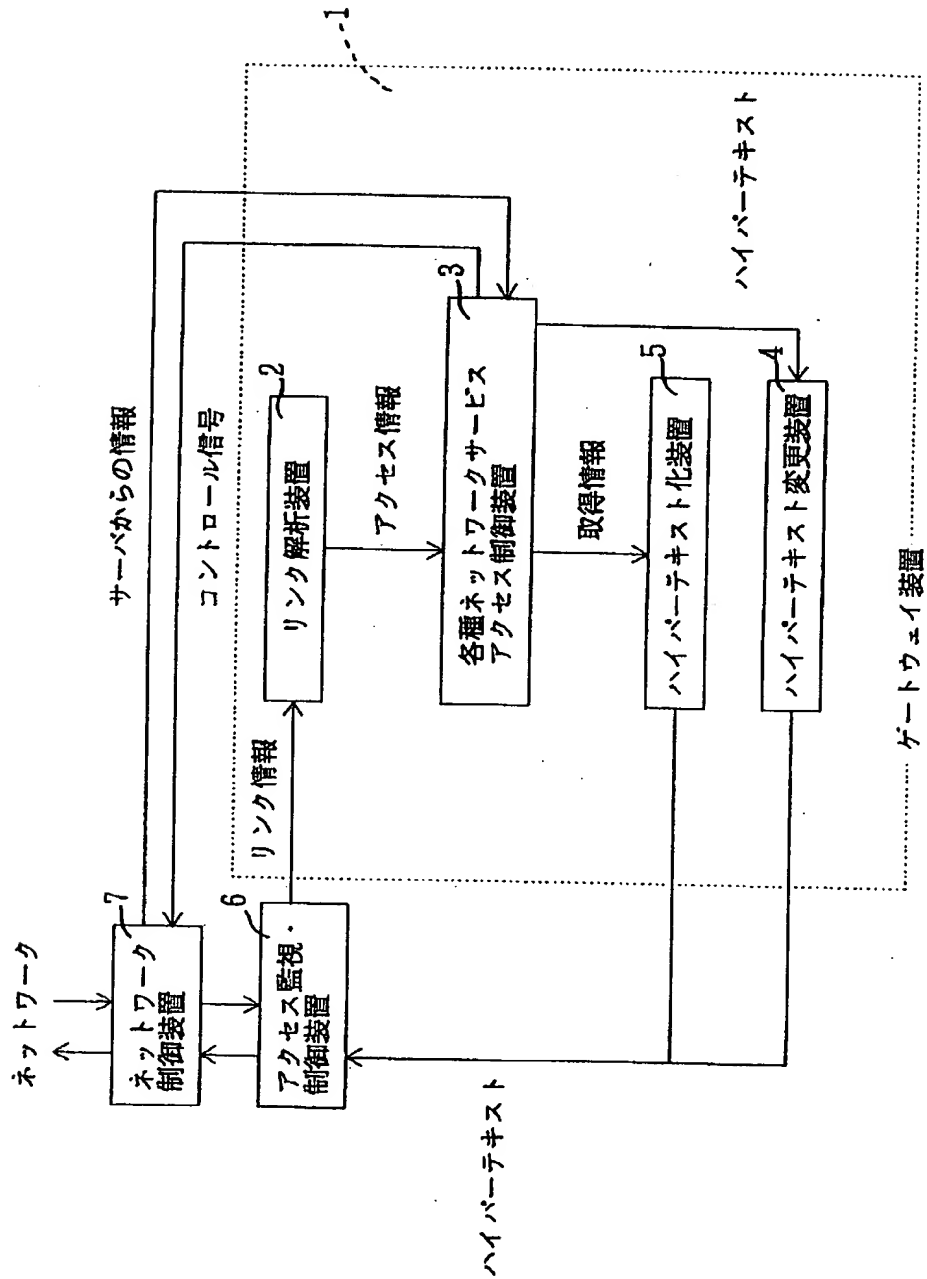
【図10】 FIG. 10

従来例2の説明図



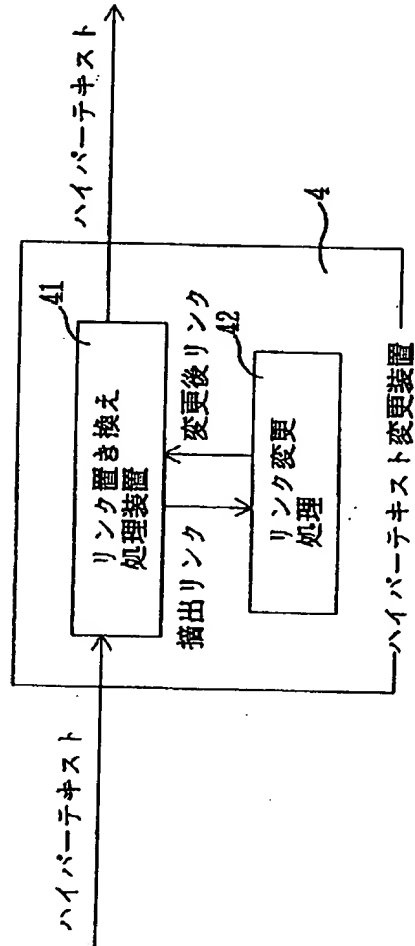
【図2】 FIG. 2

ゲートウェイ装置の構成図



【図 3】 FIG. 3

ハイパーテキスト変更装置の説明図

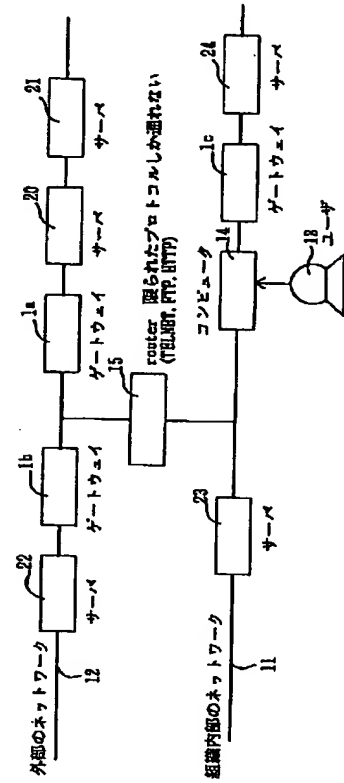
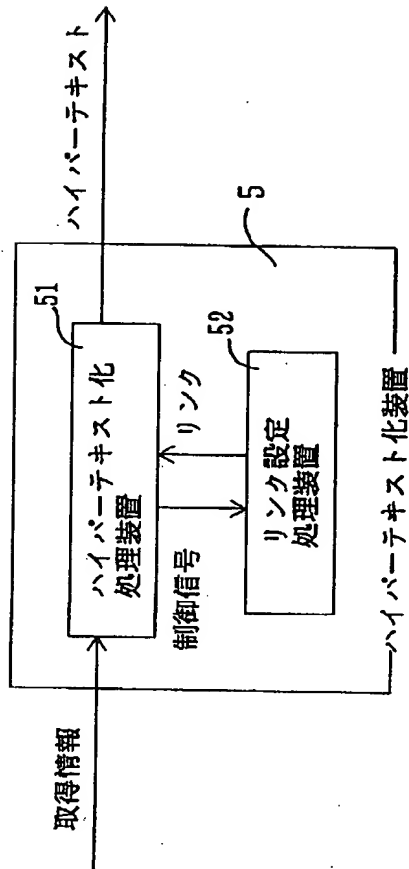


【図 4】 FIG. 4

【図 6】 FIG. 6

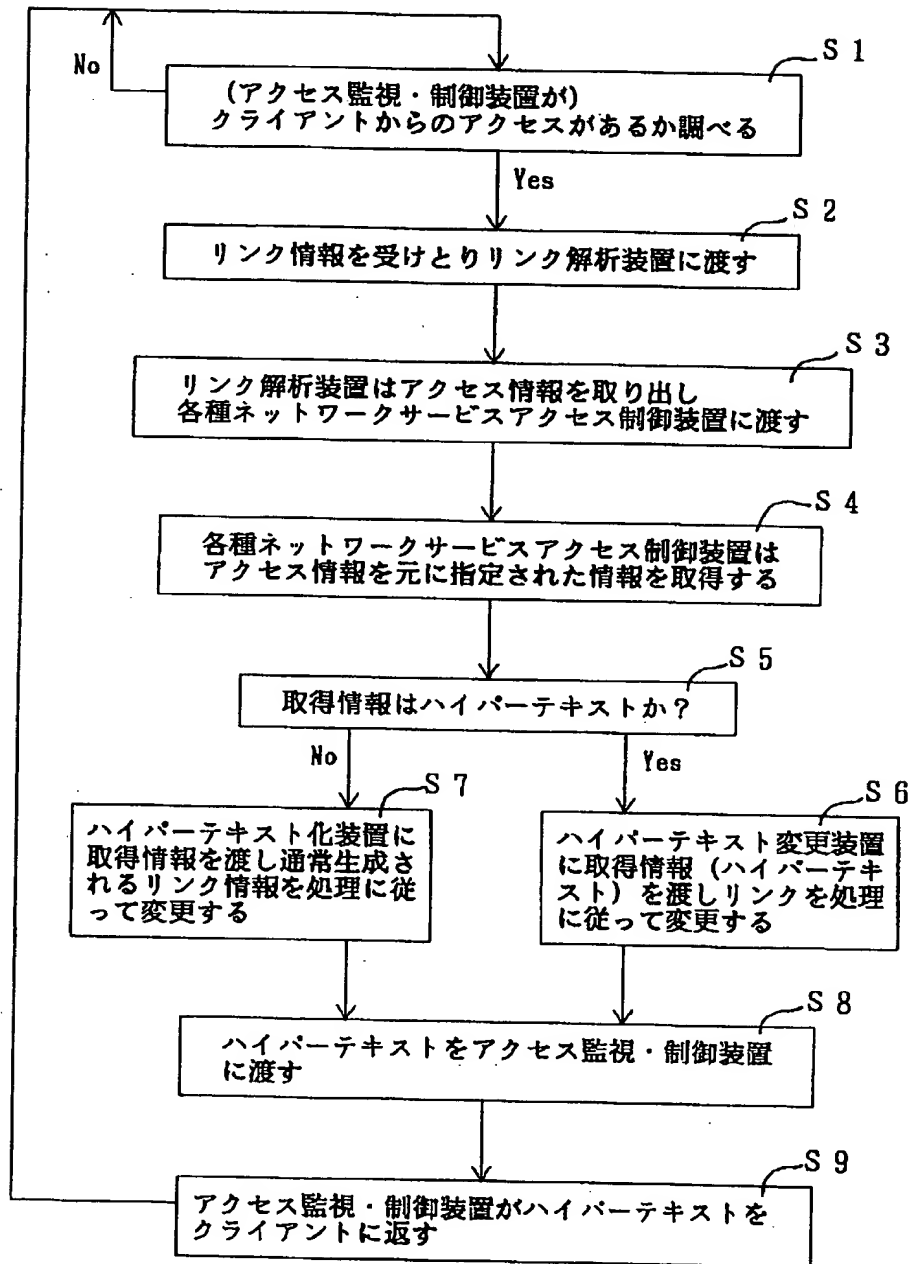
ハイパーテキスト化装置の説明図

実施例におけるサーバアクセス説明図



【図 5】 Fig. 5

実施例におけるフローチャート



【図 7】 *Fig. 7*

サーバアクセスの具体例の説明図

